

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-83297

(43) 公開日 平成10年(1998) 3月31日

(51) Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 9/06	5 5 0		G 0 6 F 9/06	5 5 0 G
12/14	3 2 0		12/14	3 2 0 E

審査請求 未請求 請求項の数9 O L (全 11 頁)

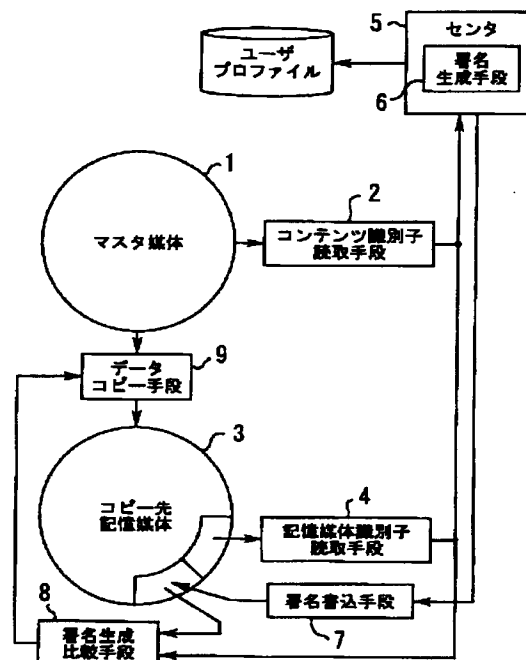
(21) 出願番号	特願平9-120523	(71) 出願人	000005223 富士通株式会社 神奈川県川崎市中原区上小田中4丁目1番1号
(22) 出願日	平成9年(1997) 5月12日	(72) 発明者	秋山 良太 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
(31) 優先権主張番号	特願平8-124823	(72) 発明者	吉岡 誠 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
(32) 優先日	平8(1996) 5月20日	(72) 発明者	内田 好昭 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
(33) 優先権主張国	日本 (J P)	(74) 代理人	弁理士 服部 毅蔵

(54) 【発明の名称】 ソフトウェアコピー処理装置、ソフトウェアコピー処理方法およびソフトウェアをコピーするプログラムを記録したコンピュータ読み取り可能な記録媒体

(57) 【要約】

【課題】 ソフトウェアコピー処理装置に関し、マスタ媒体に記憶された著作権保護ソフトウェアをユーザの記憶媒体に正当にコピーできるようにすることを目的とする。

【解決手段】 コンテンツ識別子読取手段2がマスタ媒体1上のソフトウェアの識別子を、記憶媒体識別子読取手段4がコピー先記憶媒体3の識別子をそれぞれ読み取り、コピー権販売を管理するセンタ5に送る。センタ5では署名生成手段6が送られた識別子の情報から署名を生成し、ユーザに送る。送られた署名は署名書込手段7によりコピー先記憶媒体3に書き込まれる。署名生成比較手段8はセンタ5に送った識別子の情報からユーザ側で署名を生成し、この生成した署名とコピー先記憶媒体3に書き込まれた署名とを比較し、署名が一致した場合のみ、データコピー手段9がマスタ媒体1のコピー対象ソフトウェアを読み出してコピー先記憶媒体3にコピーする。



(2)

特開平10-83297

1

【特許請求の範囲】

【請求項1】 マスタ媒体に記録されたソフトウェアをコピー先記憶媒体にコピーするソフトウェアコピー処理装置において、

個々のソフトウェアに対応してマスタ媒体に記録されたソフトウェア個別の第1の識別子の情報を読み取るコンテンツ識別子読取手段と、

コピー先記憶媒体毎に個別に記録された第2の識別子の情報を読み取る記憶媒体識別子読取手段と、

コピー権の販売を管理するセンタにおいて前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った第1および第2の識別子の情報を受けてコピー対象ソフトウェアのコピー権を認証した第1の署名を生成する署名生成手段と、

前記署名生成手段において生成された前記第1の署名を前記コピー先記憶媒体に書き込む署名書込手段と、

前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った前記第1および第2の識別子の情報から検証用の第2の署名を生成するとともに前記コピー先記憶媒体に書き込まれた第1の署名を読み出して前記第2の署名と比較して一致するかどうかを判定する署名生成比較手段と、

前記署名生成比較手段における比較の結果、第1および第2の署名が一致した場合にマスタ媒体におけるコピー対象ソフトウェアを読み取ってコピー先記憶媒体に書き込むデータコピー手段とを備えていることを特徴とするソフトウェアコピー処理装置。

【請求項2】 前記署名生成手段は、前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った前記第1および第2の識別子の情報をセンタが管理している認証鍵で暗号化した認証子を前記第1の署名として出力する署名処理手段と、前記署名処理手段で使用された認証鍵を前記センタに登録されているユーザ個別鍵で暗号化して前記認証子とともに出力する暗号化手段とを有していることを特徴とする請求項1記載のソフトウェアコピー処理装置。

【請求項3】 前記署名生成比較手段は、前記署名生成手段にて暗号化された認証鍵を前記センタに登録したユーザ個別鍵で復号して認証鍵を出力する復号手段と、前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った第1および第2の識別子の情報を前記復号手段が復号した認証鍵で暗号化して検証用の認証子を前記第2の署名として出力する認証子生成手段と、前記検証用の認証子と前記コピー先記憶媒体に第1の署名として書き込まれた認証子とを比較する比較手段とを有することを特徴とする請求項2記載のソフトウェアコピー処理装置。

【請求項4】 マスタ媒体に記録されたソフトウェアをコピー先記憶媒体にコピーするソフトウェアコピー処理方法において、

2

マスタ媒体に記録されたコピー対象データのコンテンツ識別子とコピー先記憶媒体に固有の記憶媒体識別子とをコピー権要求情報と一緒にエンドユーザからコピー権を販売するセンタに送り、

前記センタでは受けた前記コンテンツ識別子および記憶媒体識別子をセンタの認証鍵にて署名処理をして第1の認証子を生成するとともに前記認証鍵をユーザ個別鍵で暗号化処理して暗号化認証鍵を生成し、

生成された前記第1の認証子および暗号化認証鍵をエンドユーザに送り、

エンドユーザでは受けた前記第1の認証子および暗号化認証鍵を前記コピー先記憶媒体に書き込み、

前記コピー先記憶媒体に書き込まれた暗号化認証鍵をユーザ個別鍵で復号処理して前記センタで暗号化された認証鍵を取得し、

復号された認証鍵を使って前記コンテンツ識別子と記憶媒体識別子とを署名処理して検証用の第2の認証子を生成し、

生成された検証用の第2の認証子と前記コピー先記憶媒体に書き込まれた前記第1の認証子とを比較し、

前記コピー先記憶媒体に書き込まれた前記第1の認証子と前記検証用の第2の認証子とが一致した場合に、前記マスタ媒体のコピー対象データを読み出して前記コピー先記憶媒体に書き込む、

ことからなるソフトウェアコピー処理方法。

【請求項5】 マスタ媒体に記録されたソフトウェアをコピー先記憶媒体にコピーするソフトウェアコピー処理装置において、

個々のソフトウェアに対応してマスタ媒体に記録されたソフトウェア個別の第1の識別子の情報を読み取るコンテンツ識別子読取手段と、

コピー先記憶媒体毎に個別に記録された第2の識別子の情報を読み取る記憶媒体識別子読取手段と、

コピー権の販売を管理するセンタにおいて前記コンテンツ識別子読取手段が読み取った第1の識別子の情報から記憶媒体用変換鍵を生成するとともに前記記憶媒体識別子読取手段が読み取った第2の識別子の情報からマスタ媒体用変換鍵を生成し、生成した前記記憶媒体用変換鍵およびマスタ媒体用変換鍵を前記第2の識別子の情報で暗号化する変換鍵生成手段と、

前記変換鍵生成手段より出力された暗号化記憶媒体用変換鍵を前記コピー先記憶媒体に書き込む変換鍵書込手段と、

前記変換鍵生成手段より出力された暗号化記憶媒体用変換鍵および暗号化マスタ媒体用変換鍵を前記記憶媒体識別子読取手段が読み取った前記第2の識別子の情報で復号処理する変換鍵復号手段と、

前記マスタ媒体に記録されたコピー対象ソフトウェアを読み出し、前記変換鍵復号手段で復号された前記マスタ媒体用変換鍵で復号して平文のデータを出力するデータ

3

復号手段と、  
前記平文のデータを前記変換鍵復号手段で復号された前記記憶媒体用変換鍵で暗号化して前記コピー先記憶媒体に書き込むデータ書込手段と、  
を備えていることを特徴とするソフトウェアコピー処理装置。

【請求項6】 前記変換鍵生成手段は、前記コンテンツ識別子読取手段が読み取った第1の識別子の情報をセンタが管理しているマスタ鍵で暗号化して記憶媒体用変換鍵を生成する第1の暗号化手段と、前記記憶媒体識別子読取手段が読み取った第2の識別子の情報を前記マスタ鍵で暗号化してマスタ媒体用変換鍵を生成する第2の暗号化手段と、前記記憶媒体用変換鍵およびマスタ媒体用変換鍵を前記第2の識別子の情報で暗号化する第3の暗号化手段とを有することを特徴とする請求項5記載のソフトウェアコピー処理装置。

【請求項7】 ソフトウェアを識別するコンテンツ識別子とコピー権を販売するセンタが管理しているマスタ鍵とから作られたマスタ媒体用変換鍵によって暗号化されてマスタ媒体に記録されているソフトウェアをコピー先記憶媒体にコピーするソフトウェアコピー処理方法において、  
マスタ媒体に記録されたコピー対象データのコンテンツ識別子とコピー先記憶媒体に固有の記憶媒体識別子とをエンドユーザから前記センタに送り、  
前記センタでは受けた前記コンテンツ識別子および記憶媒体識別子をセンタのマスタ鍵で暗号化してマスタ媒体用変換鍵および記憶媒体用変換鍵を生成し、  
前記マスタ媒体用変換鍵および記憶媒体用変換鍵をそれぞれ前記記憶媒体識別子で暗号化し、  
暗号化された前記マスタ媒体用変換鍵および記憶媒体用変換鍵をエンドユーザに送り、  
エンドユーザでは受けた暗号化記憶媒体用変換鍵を前記コピー先記憶媒体に書き込み、  
受けた暗号化マスタ媒体用変換鍵および暗号化記憶媒体用変換鍵を前記記憶媒体識別子で復号し、  
前記マスタ媒体のコピー対象データを前記マスタ媒体用変換鍵で復号して平文のデータにし、  
前記平文のデータを前記記憶媒体用変換鍵で暗号化し、  
暗号化されたデータを前記コピー先記憶媒体に書き込む、  
ことからなるソフトウェアコピー処理方法。

【請求項8】 コンピュータを、  
個々のソフトウェアに対応してマスタ媒体に記録されたソフトウェア個別の第1の識別子の情報を読み取るコンテンツ識別子読取手段、  
コピー先記憶媒体毎に個別に記録された第2の識別子の情報を読み取る記憶媒体識別子読取手段、  
前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った第1および第2の識別

(3)

特開平10-83297

4

子の情報をコピー権の販売を管理するセンタに送る送出手段、

前記第1および第2の識別子の情報から生成されたコピー対象ソフトウェアのコピー権を認証した第1の署名を前記センタから受け取る受信手段、

前記センタから受け取った前記第1の署名を前記コピー先記憶媒体に書き込む署名書込手段、

前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った前記第1および第2の

10 識別子の情報から検証用の第2の署名を生成するとともに前記コピー先記憶媒体に書き込まれた第1の署名を読み出して前記第2の署名と比較して一致するかどうかを判定する署名生成比較手段、および前記署名生成比較手段における比較の結果、第1および第2の署名が一致した場合にマスタ媒体におけるコピー対象ソフトウェアを読み取ってコピー先記憶媒体に書き込むデータコピー手段として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項9】 コンピュータを、

20 個々のソフトウェアに対応してマスタ媒体に記録されたソフトウェア個別の第1の識別子の情報を読み取るコンテンツ識別子読取手段、

コピー先記憶媒体毎に個別に記録された第2の識別子の情報を読み取る記憶媒体識別子読取手段、

前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った第1および第2の識別子の情報をコピー権の販売を管理するセンタに送る送出手段、

第1の識別子の情報から生成された記憶媒体用変換鍵および第2の識別子の情報から生成されたマスタ媒体用変換鍵を前記第2の識別子の情報で暗号化した暗号化記憶媒体用変換鍵および暗号化マスタ媒体用変換鍵を前記センタから受け取る受信手段、

30 前記暗号化記憶媒体用変換鍵を前記コピー先記憶媒体に書き込む変換鍵書込手段、  
前記暗号化記憶媒体用変換鍵および暗号化マスタ媒体用変換鍵を前記記憶媒体識別子読取手段が読み取った前記第2の識別子の情報で復号処理する変換鍵復号手段、

40 前記マスタ媒体に記録されたコピー対象ソフトウェアを読み出し、前記変換鍵復号手段で復号された前記マスタ媒体用変換鍵で復号して平文のデータを出力するデータ復号手段、および前記平文のデータを前記変換鍵復号手段で復号された前記記憶媒体用変換鍵で暗号化して前記コピー先記憶媒体に書き込むデータ書込手段として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明はソフトウェアコピー処理装置、ソフトウェアコピー処理方法およびソフトウ

50

(4)

特開平10-83297

5

ウェアをコピーするプログラムを記録したコンピュータ読み取り可能な記録媒体に関し、特に著作権保護ソフトウェアをユーザの記憶媒体に正当にコピーするソフトウェアコピー処理装置、ソフトウェアコピー処理方法およびソフトウェアをコピーするプログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【0002】近年、ソフトウェアの流通形態には様々のもがあり、フロッピーディスクやCD-ROM (compact disk read only memory)、半導体メモリなどの記憶媒体にソフトウェアを記録したものを購入したり、あるいはネットワークを経由してソフトウェアをダウンロードすることによって購入したりする場合があるが、これらのソフトウェアは通常いずれも他の記憶媒体に容易にコピーが可能のため、常に不正コピーの問題があり、著作権のあるソフトウェアについては深刻である。

【0003】

【従来の技術】従来、コンピュータ用のアプリケーションプログラム、辞書データ、映像・音楽データなどのソフトウェアの販売形態の一つに、これらソフトウェアをCD-ROMに電子的に鍵をかけた状態で記録して頒布する方法がある。この場合、ユーザは、そのソフトウェアの販売を管理しているセンタに連絡して利用したいソフトウェアの購入手続きをする。その後、ユーザは、購入手続き時に渡された鍵を使って鍵付きのソフトウェアを開くことにより、それをたとえばハードディスクにインストールすることができる。

【0004】また、別の例として、書き込み可能な記憶媒体にあらかじめセンタが管理しているコピー権販売に関する識別子情報を書き込んでおく場合がある。CD-ROMに記録されたソフトウェアをコピーする場合は、その記憶媒体の販売店またはユーザがセンタに通知する。ソフトウェアの販売手続きをすることによってセンタから発行される識別子情報を記憶媒体に書き込まれた識別子情報と比較して一致する場合のみ、CD-ROMから記憶媒体にソフトウェアをコピーすることが可能になる。

【0005】

【発明が解決しようとする課題】しかし、ハードディスクなどにインストールされたソフトウェアは、通常、そのまま実行あるいは利用できる、すなわち、鍵がかけられていないので、依然として不正コピーの問題は解消されていないという問題点があった。

【0006】また、記憶媒体に識別子情報を書き込んでおく場合には、センタは記憶媒体を製造する工場と連携して識別子情報を管理する必要がある、しかも、記憶媒体についてコピー専用媒体と一般用記憶媒体とを区別して取り扱う必要があるという問題点があった。

【0007】本発明はこのような点に鑑みてなされたものであり、マスタ媒体に記憶された著作権付きのソフト

6

ウェアをリード/ライト可能なユーザの媒体識別子付き記憶媒体に正当にコピーすることができるソフトウェアコピー処理装置、ソフトウェアコピー処理方法およびソフトウェアをコピーするプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【0008】

【課題を解決するための手段】図1は上記目的を達成する本発明の原理図である。本発明のソフトウェアコピー処理装置は、マスタ媒体1に記録されたコピー対象ソフトウェアの識別子を読み取るコンテンツ識別子読取手段2と、コピー先記憶媒体3の識別子を読み取る記憶媒体識別子読取手段4と、コピー権の販売を管理するセンタ5においてコンテンツ識別子読取手段2および記憶媒体識別子読取手段4が読み取った識別子の情報からコピー権を要求したユーザにコピー権を認証した署名を生成する署名生成手段6と、生成された署名をコピー先記憶媒体3に書き込む署名書込手段7と、コピー先記憶媒体3に書き込まれた署名とユーザ側で生成した署名とを比較する署名生成比較手段8と、比較結果が一致した場合にマスタ媒体1のコピー対象ソフトウェアをコピー先記憶媒体3にコピーするデータコピー手段9とから構成されている。

【0009】上記の構成によれば、まず、コンテンツ識別子読取手段2がマスタ媒体1からソフトウェアのコンテンツ識別子を読み取り、記憶媒体識別子読取手段4がコピー先記憶媒体3からその記憶媒体識別子を読み取る。これらの識別子の情報は、センタに送られる。センタ5では、送られた識別子の情報から署名生成手段6が署名を生成してユーザに送り返す。その署名は、署名書込手段7によりコピー先記憶媒体3に書き込まれる。署名生成比較手段8は、コンテンツ識別子読取手段2および記憶媒体識別子読取手段4で読み取った識別子の情報から内部的に署名を生成してコピー先記憶媒体3に書き込まれた署名と比較する。この署名の比較が一致した場合は、データコピー手段9がマスタ媒体1から暗号化されたコピー対象ソフトウェアをそのままコピー先記憶媒体3にコピーする。

【0010】また、本発明によれば、マスタ媒体に記録されたソフトウェアをコピー先記憶媒体にコピーするソフトウェアコピー処理方法において、マスタ媒体に記録されたコピー対象データのコンテンツ識別子とコピー先記憶媒体に固有の記憶媒体識別子とをコピー権要求情報と一緒にエンドユーザからコピー権を販売するセンタに送り、前記センタでは受けた前記コンテンツ識別子および記憶媒体識別子をセンタの認証鍵にて署名処理をして第1の認証子を生成するとともに前記認証鍵をユーザ個別鍵で暗号化処理して暗号化認証鍵を生成し、生成された前記第1の認証子および暗号化認証鍵をエンドユーザに送り、エンドユーザでは受けた前記第1の認証子およ

(5)

特開平10-83297

7

び暗号化認証鍵を前記コピー先記憶媒体に書き込み、前記コピー先記憶媒体に書き込まれた暗号化認証鍵をユーザ個別鍵で復号処理して前記センタで暗号化された認証鍵を取得し、復号された認証鍵を使って前記コンテンツ識別子と記憶媒体識別子とを署名処理して検証用の第2の認証子を生成し、生成された検証用の第2の認証子と前記コピー先記憶媒体に書き込まれた前記第1の認証子とを比較し、前記コピー先記憶媒体に書き込まれた前記第1の認証子と前記検証用の第2の認証子とが一致した場合に、前記マスタ媒体のコピー対象データを読み出して前記コピー先記憶媒体に書き込む、ことからなるソフトウェアコピー処理方法が提供される。

【0011】さらに、本発明によれば、コンピュータを、個々のソフトウェアに対応してマスタ媒体に記録されたソフトウェア個別の第1の識別子の情報を読み取るコンテンツ識別子読取手段、コピー先記憶媒体毎に個別に記録された第2の識別子の情報を読み取る記憶媒体識別子読取手段、前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った第1および第2の識別子の情報をコピー権の販売を管理するセンタに送る送出手段、前記第1および第2の識別子の情報から生成されたコピー対象ソフトウェアのコピー権を認証した第1の署名を前記センタから受け取る受信手段、前記センタから受け取った前記第1の署名を前記コピー先記憶媒体に書き込む署名書込手段、前記コンテンツ識別子読取手段および前記記憶媒体識別子読取手段がそれぞれ読み取った前記第1および第2の識別子の情報から検証用の第2の署名を生成するとともに前記コピー先記憶媒体に書き込まれた第1の署名を読み出して前記第2の署名と比較して一致するかどうかを判定する署名生成比較手段、および前記署名生成比較手段における比較の結果、第1および第2の署名が一致した場合にマスタ媒体におけるコピー対象ソフトウェアを読み取ってコピー先記憶媒体に書き込むデータコピー手段として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体が提供される。

【0012】この記録媒体は、好ましくは、ソフトウェアを記録しているマスタ媒体と同じ媒体とすることができる。コンピュータが記録媒体からコンテンツ識別子読取手段を読み出して実行することでマスタ媒体からソフトウェア個別の第1の識別子の情報が読み取られ、記憶媒体識別子読取手段4によりコピー先記憶媒体からコピー先記憶媒体毎に個別に記録された第2の識別子の情報が読み取られる。これらの識別子の情報は、送出手段によりコピー権の販売を管理するセンタに送られる。続いて、受信手段によりセンタからソフトウェアのコピー権を認証した第1の署名を受け取ると、署名書込手段がその第1の署名をコピー先記憶媒体に書き込む。次に、署名生成比較手段により、第1および第2の識別子の情報から内部的に第2の署名を生成してコピー先記憶媒体に

8

書き込まれた第1の署名と比較し、これらの署名が一致した場合に、データコピー手段によりソフトウェアをマスタ媒体からコピー先記憶媒体にコピーする。

【0013】

【発明の実施の形態】まず、本発明の概略について図面を参照して説明する。図1は本発明のソフトウェアコピー処理装置の原理構成を示す図である。

【0014】この図において、本発明のソフトウェアコピー処理装置は、マスタ媒体1に記録されたコピー対象ソフトウェアのソフトウェア個別の識別情報を読み取るコンテンツ識別子読取手段2と、コピー先記憶媒体3の個別の識別情報を読み取る記憶媒体識別子読取手段4と、コピー権の販売を管理するセンタ5においてコンテンツ識別子読取手段2および記憶媒体識別子読取手段4がそれぞれ読み取った識別情報を受けてコピー対象ソフトウェアのコピー権を認証した署名を生成する署名生成手段6と、この署名生成手段6で生成された署名をコピー先記憶媒体3に書き込む署名書込手段7と、コンテンツ識別子読取手段2および記憶媒体識別子読取手段4がそれぞれ読み取った識別情報から署名を生成してこれとコピー先記憶媒体3に書き込まれた署名とを比較して一致するかどうかを判定する署名生成比較手段8と、この署名生成比較手段8にて署名が一致した場合にマスタ媒体1におけるコピー対象ソフトウェアを読み取ってコピー先記憶媒体3に書き込むデータコピー手段9とから構成されている。

【0015】マスタ媒体1は販売対象のソフトウェアが暗号化されて記録されており、各ソフトウェアにはコンテンツ識別子が付けられている。また、コピー先記憶媒体3はその工場出荷時にあらかじめ個別の記憶媒体識別子が付けられているとする。ここで、ユーザがマスタ媒体1に記録されているソフトウェアの中からコピー対象ソフトウェアを指定すると、コンテンツ識別子読取手段2がマスタ媒体1からそのソフトウェアに対応するコンテンツ識別子を読み取り、記憶媒体識別子読取手段4がコピー先記憶媒体3からその記憶媒体識別子を読み取る。これら識別子の情報はコピー権購入の要求と一緒にセンタ5に送られる。センタ5では、署名生成手段6が受けたコンテンツ識別子および記憶媒体識別子の情報からコピー権を認証した署名を生成して、ユーザに送り返す。センタ5は、また、署名生成の際に、ユーザプロフィールに対してユーザの登録処理および課金処理を行う。

【0016】ユーザ側では、署名書込手段7が署名生成手段6より送られて来た署名を受けて、これをコピー先記憶媒体3に書き込む。次いで、署名生成比較手段8においては、まず、コンテンツ識別子読取手段2により読み取られたコンテンツ識別子と記憶媒体識別子読取手段4により読み取られた記憶媒体識別子とから内部的に署名を生成し、次に、この生成された署名とコピー先記憶

10

20

30

40

50

(6)

特開平10-83297

9

媒体3に書き込まれた署名とを比較して一致しているかどうかを判定する。署名生成比較手段8における署名の比較が一致した場合は、データコピー手段9がマスタ媒体1から暗号化されているコピー対象ソフトウェアを読み取ってコピー先記憶媒体3に書き込む。ユーザがコピー先記憶媒体3に書き込まれたソフトウェアを利用する場合は、そのソフトウェアを復号しながらこのソフトウェアを実行する処理装置のメインメモリに展開して実行することになる。

【0017】次に、本発明の実施の形態を、CD-ROMにて配付された著作権保護ソフトウェアをMO(magneto-optical disc:光磁気ディスク)媒体にコピーする場合を例にして説明する。

【0018】図2はソフトウェアコピー処理装置の処理の流れを示すフローチャートである。本発明のソフトウェアコピー処理装置において、CD-ROMに記録されたソフトウェアをMO媒体にコピーする場合には、まず、エンドユーザ側にて、MO媒体の記憶媒体個別識別子IDkおよびCD-ROMのコピーを希望するソフトウェアのソフトウェア個別識別子SIDIを、コピー権の販売を管理しているセンタに送信する(ステップS1)。次いで、センタ側では、コピー権販売の手続き処理を行うとともに、受信された記憶媒体個別識別子IDkおよびソフトウェア個別識別子SIDIから認証子CSを生成してエンドユーザ側に送り返す(ステップS2)。エンドユーザ側では、受信した認証子CSをMO媒体の所定の記憶領域に書き込む(ステップS3)。ここで、エンドユーザ側においても、センタに送信した記憶媒体個別識別子IDkおよびソフトウェア個別識別子SIDIを使って検証用の認証子CS'を生成する(ステップS4)。そして、エンドユーザ側で生成した認証子CS'とMO媒体に書き込まれた認証子CSとを比較する(ステップS5)。これら認証子CS'およびCSの比較の結果、両認証子が一致しているかどうかを判定され(ステップS6)、ここで、一致している場合には、CD-ROMからソフトウェア個別識別子SIDIを有するソフトウェアの暗号化データをMO媒体に書き込む(ステップS7)。もし、ステップS6に判定において、両認証子が一致していない場合には、CD-ROMからMO媒体へのソフトウェアの書き込みは行われずに終了する。

【0019】図3はCD-ROMおよびMO媒体の構成を示す図である。この図において、(A)はCD-ROM11の構成を示したもので、このCD-ROM11には、それぞれソフトウェア個別識別子SIDI(i=1, 2, ..., n)を有する著作権保護ソフトウェアと、CD-ROMからMO媒体への著作権保護ソフトウェアのコピー操作を行うマネージャアプリケーションソフトウェアMAとが記録されている。各著作権保護ソフトウェアはそれぞれ暗号化された状態で記録されてい

10

る。マネージャアプリケーションソフトウェアMAは、CD-ROMからMO媒体へソフトウェアをコピーする場合に、エンドユーザ側のたとえばパーソナルコンピュータのような端末の本体に読み込まれて実行され、図2の処理のうちエンドユーザ側の処理を行う。

【0020】また、(B)はMO媒体12の構成を示したもので、このMO媒体12には、記憶媒体個別識別子IDk(k=1, 2, ..., m)が記録されている。MO媒体12はユーザが自由にデータを書き込んだり、消去することができる記憶領域を有しているが、MO媒体12の記憶媒体個別識別子IDkが書き込まれている領域は、読み出しは可能であるが書き換えは不可能な領域である。この記憶媒体個別識別子IDkは、たとえば工場出荷時にそれぞれのMO媒体に付けられるシリアル番号とすることができる。

【0021】次に、CD-ROMの著作権保護ソフトウェアをMO媒体にコピーする具体的な手順について説明する。図4は著作権保護ソフトウェアのコピー処理の手順を示す図である。

【0022】この図において、コピー処理の手順を、たとえばパーソナルコンピュータで構成の本体側の処理とコピー権の販売を管理しているセンタ側の処理とに分けて示してあり、ここでは、本体側を「エンドユーザ」、センタ側を「センタ」で示し、それらの間は「通信路/運搬路」で示してある。

【0023】ここで、エンドユーザの端末はCD-ROMドライブ装置およびMOドライブ装置を備え、CD-ROMドライブ装置には、著作権保護ソフトウェアが記録されたマスタ媒体であるCD-ROM11が装填されており、MOドライブ装置にはコピー先の媒体であるMO媒体12が装填されているものとする。そして、CD-ROM11のコピー対象ソフトウェアはソフトウェア個別識別子SIDIを有するソフトウェアであり、MO媒体12に固有の識別子は記憶媒体個別識別子IDkであるとする。

【0024】まず、エンドユーザの本体側処理では、CD-ROM11のマネージャアプリケーションソフトウェアMAを起動して、コピー対象ソフトウェアが指定されると、CD-ROM11からそのソフトウェアのソフトウェア個別識別子SIDIが読み取られ、MO媒体12から記憶媒体個別識別子IDkが読み取られる。これらソフトウェア個別識別子SIDIおよび記憶媒体個別識別子IDkは、コピー権要求情報を含む要求文とともにセンタに送信される。

【0025】センタ側では、受信したエンドユーザからの情報の要求内容をまず、ユーザプロファイル13に書き込む。さらに、受信したソフトウェア個別識別子SIDIおよび記憶媒体個別識別子IDkは署名処理装置14に入力される。この署名処理装置14は、秘密鍵であるセンタの認証鍵KEYcを使ってデータ圧縮処理を行

(7)

特開平10-83297

11

い、認証子CSを出力する。この認証子CSが署名の役割を果たす。次に、署名処理装置14で使用した認証鍵KEYcは暗号化装置15に入力され、ユーザ個別鍵KUで暗号化されて、暗号化電文EKU(KEYc)として出力される。署名処理装置14より出力された認証子CSおよび暗号化装置15より出力された暗号化電文EKU(KEYc)は、センタ識別子IDcとともにエンドユーザに送り返される。

【0026】エンドユーザ側では、センタより送られた情報のうち、認証子CSおよび暗号化電文EKU(KEYc)はコピー先のMO媒体12上に一度書き込まれ、そしてこの書き込まれた媒体上の認証子CSおよび暗号化電文EKU(KEYc)がマネージャアプリケーションへ渡される。

【0027】本体側処理では、署名検証のために、まず、渡された暗号化電文EKU(KEYc)が復号装置16に入力され、ユーザ個別鍵KUを使用して復号されることにより、センタにおいて暗号化された認証鍵KEYcが取り出される。次いで、署名処理装置17において、CD-ROM11から読み取ったソフトウェア個別識別子SIDiおよびMO媒体12から読み取った記憶媒体個別識別子IDkから、復号装置16において復号された認証鍵KEYcを使って、エンドユーザ側で検証用の認証子CS'を生成する。その後、MO媒体12上に書き込まれた認証子CSと署名処理装置17で生成された認証子CS'とが比較器18で比較される。比較器18での比較の結果、認証子CSと認証子CS'とが一致すれば、スイッチ19が作動して、ソフトウェア個別識別子SIDiを有するコピー対象ソフトウェアが暗号化データの状態で、コピー先のMO媒体12に書き込まれる。

【0028】ここで、センタ側の署名処理装置14およびエンドユーザ側の署名処理装置17における処理の例について以下に説明する。図5は署名処理装置の構造例を示す図である。

【0029】署名処理装置は、ソフトウェア個別識別子SIDiおよび記憶媒体個別識別子IDkと認証子CSとを受けて排他的論理和处理を行う排他的論理和处理部21と、この排他的論理和处理部21の出力とセンタの認証鍵KEYcとを入力して認証子CSを出力する暗号化処理部22とからなり、ハッシュ関数を構成している。

【0030】まず、入力されたソフトウェア個別識別子SIDiおよび記憶媒体個別識別子IDkデータは、暗号化処理部22においてブロック単位で認証鍵KEYcにより暗号化される。暗号化処理部22で暗号化処理された出力データは入力側に帰還されて、排他的論理和处理部21において次のブロックデータと排他的論理和处理され、暗号化処理部22で再び暗号化される。このような処理は、最終のブロックが入力されるまで繰り返さ

12

れる。この間、処理結果は出力されず、最終ブロックが暗号化されたとき、暗号化処理部22から初めて認証子CSとして出力される。

【0031】次に、以上の手順でMO媒体12に暗号化されたままでコピーされたデータに含まれるソフトウェアのプログラムを実行する場合の処理手順について説明する。

【0032】図6はコピーされたデータに含まれるソフトウェアのプログラムの実行処理手順を示す説明図である。MO媒体12には、認証子CS、暗号化電文EKU(KEYc)、記憶媒体個別識別子IDkデータ、およびソフトウェア個別識別子SIDiが記録され、コピーされたソフトウェアは暗号化データEKd(DATA)として記録されている。この暗号化データEKd(DATA)はソフトウェアをCD-ROM11に記録する際に鍵Kdによって暗号化されたものであり、その暗号化に使用した鍵Kdはマネージャアプリケーションソフトウェアによって保持されている。

【0033】本体側処理では、まず、MO媒体12から認証子CS、暗号化電文EKU(KEYc)、記憶媒体個別識別子IDkデータ、およびソフトウェア個別識別子SIDiが読み出され、その内の暗号化電文EKU(KEYc)が復号装置16に入力され、ユーザ個別鍵KUを使用して復号されることで認証鍵KEYcが取り出される。次いで、MO媒体12から読み出したソフトウェア個別識別子SIDiおよびMO媒体12から読み取った記憶媒体個別識別子IDkを、復号装置16において復号された認証鍵KEYcを使って、検証用の認証子CS'を生成する。その後、MO媒体12上に書き込まれた認証子CSと署名処理装置17によって生成された認証子CS'とが比較器18で比較される。比較器18での比較の結果、認証子CSと認証子CS'とが一致すれば、スイッチ19が作動し、MO媒体12から読み出された暗号化ソフトウェアである暗号化データEKd(DATA)がそのスイッチ19を経由して復号装置25に入力される。復号装置25では、入力された暗号化データEKd(DATA)はマネージャアプリケーションソフトウェアが保持している鍵Kdを使って復号され、平文のデータDATAに戻される。このデータDATAは、本体側の中央処理装置(CPU)・メモリ26のメモリ上にロードされ、ここで、そのソフトウェアのプログラムはCPUによって実行処理される。

【0034】次に、本発明のソフトウェアコピー処理装置の別の実施の形態について説明する。この例では、CD-ROMに記録されたソフトウェアはソフトウェア個別識別子DIDを有し、かつ、そのソフトウェアのデータDataはソフトウェア個別識別子DIDとコピー権販売センタが管理しているマスタ鍵KMとから作られたマスタ媒体用変換鍵Kaによって暗号化され、暗号化データEKa(Data)になっているとし、MO媒体は

50

記憶媒体個別識別子M i dのシリアル番号を有しているとする。

【0035】図7はソフトウェアコピー処理装置の別のコピー処理の流れを示すフローチャートである。まず、エンドユーザ側にて、コピー先のMO媒体の記憶媒体個別識別子M i dおよびCD-ROMのコピーを希望するソフトウェアのソフトウェア個別識別子D I Dをコピー権の販売を管理しているコピー権販売センタに送信する（ステップS11）。次いで、センタ側では、受信されたソフトウェア個別識別子D I Dがセンタに登録されているかどうかの検証が行われる（ステップS12）。その後、受信された記憶媒体個別識別子M i dおよびソフトウェア個別識別子D I Dをセンタ管理のマスタ鍵K Mで暗号化して記憶媒体用変換鍵K uおよびマスタ媒体用変換鍵K aを生成する（ステップS13）。次いで、これら記憶媒体用変換鍵K uおよびマスタ媒体用変換鍵K aを記憶媒体個別識別子M i dで暗号化して暗号化電文E M i d（K u，K a）を生成し、生成した暗号化電文E M i d（K u，K a）を要求元のエンドユーザへ送り返す（ステップS14）。エンドユーザ側では、受信した暗号化電文E M i d（K u，K a）のうち、MO媒体に関連した情報を有する暗号化電文E M i d（K u）をMO媒体に書き込むとともに受信した暗号化電文E M i d（K u，K a）を記憶媒体個別識別子M i dで復号して記憶媒体用変換鍵K uおよびマスタ媒体用変換鍵K aを得る（ステップS15）。次に、ステップS15で得られたマスタ媒体用変換鍵K aを使用して、CD-ROMのソフトウェア個別識別子D I Dに対応する暗号化データE K a（D a t a）を復号し、平文のデータD a t aを得る（ステップS16）。そして、このデータD a t aをステップS15で得られた記憶媒体用変換鍵K uで再暗号化してMO媒体に書き込み、コピーを終了する（ステップS17）。

【0036】次に、CD-ROMのソフトウェアをMO媒体にコピーする具体的な手順について説明する。なお、エンドユーザ側でコピー権販売センタに要求を出すときに最初に行われる処理は、コピー先のMO媒体の記憶媒体個別識別子M i dおよびCD-ROMのコピー対象ソフトウェアのソフトウェア個別識別子D I Dの読み出し処理と、これら記憶媒体個別識別子M i dおよびソフトウェア個別識別子D I Dのセンタへの送信処理だけなので、この最初の処理に関する説明は省略し、センタ側の処理の説明から行う。

【0037】図8はセンタ側における処理の手順を示す説明図である。この図において、センタは、まず、回線を通じてエンドユーザから送信された記憶媒体個別識別子M i dおよびソフトウェア個別識別子D I Dを受信し、このうち、記憶媒体個別識別子M i dをセンタ管理のマスタ鍵K Mを有する暗号化装置31に入力し、ソフトウェア個別識別子D I Dを比較器32へ入力する。暗

号化装置31は記憶媒体個別識別子M i dをマスタ鍵K Mで暗号化して記憶媒体用変換鍵K uを生成する。一方、比較器32は、ソフトウェア個別識別子D I Dの正当性検証のため、発行コンテンツ識別子ファイル33を検索し、要求されたソフトウェア個別識別子D I Dと比較する。ここで、発行コンテンツ識別子ファイル33のソフトウェア個別識別子D I Dと要求されたソフトウェア個別識別子D I Dとが一致した場合には、スイッチ34は閉成状態に制御される。すると、要求されたソフトウェア個別識別子D I Dはマスタ鍵K Mを有する暗号化装置35に入力される。暗号化装置35はソフトウェア個別識別子D I Dをマスタ鍵K Mで暗号化してマスタ媒体用変換鍵K aを生成する。暗号化装置31で生成された記憶媒体用変換鍵K uおよび暗号化装置35で生成されたマスタ媒体用変換鍵K aは暗号化装置36に入力され、それぞれ記憶媒体個別識別子M i dによって暗号化される。暗号化装置36によって暗号化された暗号化電文E M i d（K u，K a）は回線を通じて要求元のエンドユーザに送信される。この処理が達成されると、ユーザプロファイル37に課金処理の指示が伝えられ、要求元のエンドユーザに対して課金が実施される。

【0038】図9はエンドユーザ側における処理の手順を示す説明図である。この図において、センタから送信された暗号化電文E M i d（K u，K a）を受信すると、まず、そのうちのMO媒体に関する暗号化電文E M i d（K u）をMO媒体40の所定の領域41に書き込む。そして、受信された暗号化電文E M i d（K u，K a）は復号装置51に入力される。復号装置51はMO媒体40の記憶媒体個別識別子M i dを使って暗号化電文E M i d（K u，K a）を復号し、記憶媒体用変換鍵K uおよびマスタ媒体用変換鍵K aを出力する。復号されたマスタ媒体用変換鍵K aは復号装置52に復号鍵として入力され、記憶媒体用変換鍵K uは暗号化装置53に暗号鍵として入力される。まず、復号装置52は、CD-ROM60のソフトウェア個別識別子D I Dに対応する暗号化データE K a（D a t a）を読み込んでマスタ媒体用変換鍵K aにより復号し、平文のデータD a t aに戻して出力する。このデータD a t aは暗号化装置53に入力され、記憶媒体用変換鍵K uで再暗号化される。暗号化装置53で暗号化された暗号化データE K u（D a t a）はMO媒体40に書き込まれる。

【0039】次に、以上の手順でMO媒体40に書き込まれた、このMO媒体40に固有の識別子およびセンタのマスタ鍵に基づく変換鍵による暗号化データE K u（D a t a）を利用する場合の処理手順について説明する。

【0040】図10はコピーされたデータの利用処理手順を示す説明図である。MO媒体40は、書き換え可能な領域の中の領域41に暗号化電文E M i d（K u）が記憶され、書き換え不可能な領域42に記憶媒体個別識



(9)

特開平10-83297

15

別子Midが記憶され、それ以外の領域の一部にコピーされた暗号化データEKu(Data)が記憶されている。ここで、暗号化データEKu(Data)を利用する場合は、まず、MO媒体40上の記憶媒体個別識別子Midおよび暗号化電文EMid(Ku)が読み出されて復号装置54に入力される。復号装置54は記憶媒体個別識別子Midを用いて暗号化電文EMid(Ku)を復号し、記憶媒体用変換鍵Kuを出力する。復号装置55は記憶媒体用変換鍵Kuを復号鍵として使用し、MO媒体40から読み出された暗号化データEKu(Data)を復号して、平文のデータDataを出力する。このデータDataはエンドユーザの端末であるパーソナルコンピュータのメインメモリ上に展開され、これがプログラムならば実行され、辞書データならば検索するなどして利用される。

【0041】

【発明の効果】以上説明したように本発明では、マスタ媒体のコピー対象データの識別子およびコピー先記憶媒体の識別子の情報から署名を生成する署名生成手段をセンタ側に備え、エンドユーザ側では署名生成手段によって生成された署名をコピー先記憶媒体に書き込む署名書込手段と、エンドユーザ側で生成した検証用の署名とコピー先記憶媒体に書き込まれた署名とを比較する署名生成比較手段と、比較結果によってマスタ媒体のコピー対象データをコピー先記憶媒体に書き込むデータコピー手段を備えるように構成した。このため、センタは、コピー先記憶媒体の識別子の情報に対してこれと対応する署名を発行するだけでよく、また、コピー先記憶媒体の製造工場と連携しての識別子情報の管理というようなことも必要なく、コピー先記憶媒体を製造する工場やこれを販売する店において、コピー先記憶媒体の在庫管理を不\*

16

\* 要にすることができる。

【図面の簡単な説明】

【図1】本発明のソフトウェアコピー処理装置の原理構成を示す図である。

【図2】ソフトウェアコピー処理装置の処理の流れを示すフローチャートである。

【図3】CD-ROMおよびMO媒体の構成を示す図である。

【図4】著作権保護ソフトウェアのコピー処理の手順を示す図である。

【図5】署名処理装置の構造例を示す図である。

【図6】コピーされたデータに含まれるソフトウェアのプログラムの実行処理手順を示す説明図である。

【図7】ソフトウェアコピー処理装置の別のコピー処理の流れを示すフローチャートである。

【図8】センタ側における処理の手順を示す説明図である。

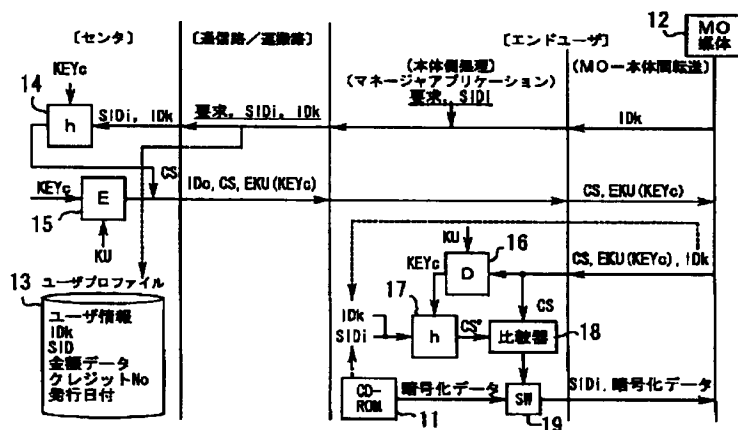
【図9】エンドユーザ側における処理の手順を示す説明図である。

【図10】コピーされたデータの利用処理手順を示す説明図である。

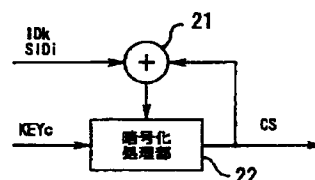
【符号の説明】

- 1 マスタ媒体
- 2 コンテンツ識別子読取手段
- 3 コピー先記憶媒体
- 4 記憶媒体識別子読取手段
- 5 センタ
- 6 署名生成手段
- 7 署名書込手段
- 8 署名生成比較手段
- 9 データコピー手段

【図4】



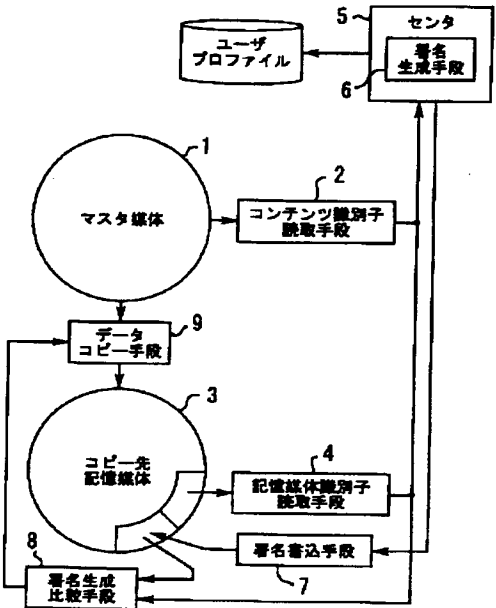
【図5】



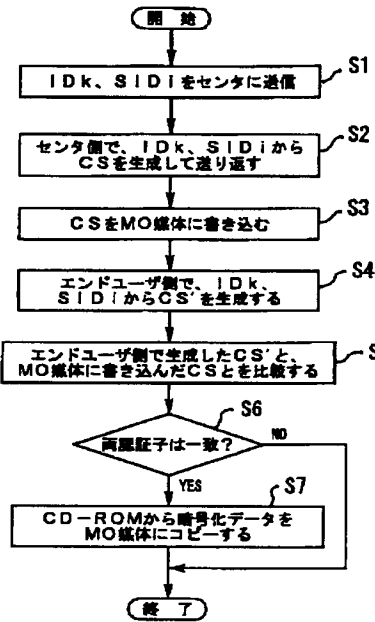
(10)

特開平10-83297

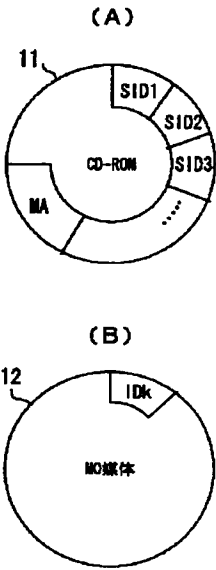
【図1】



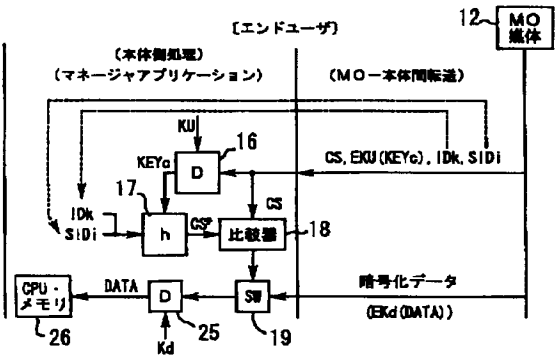
【図2】



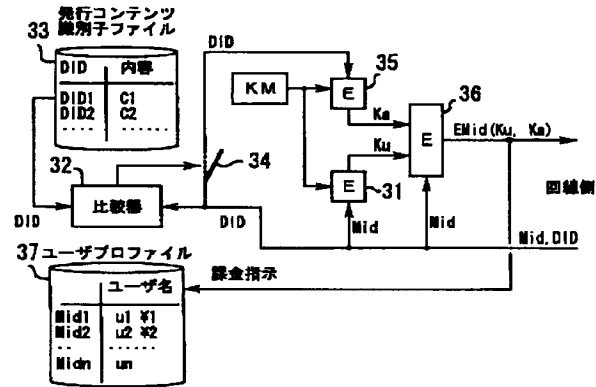
【図3】



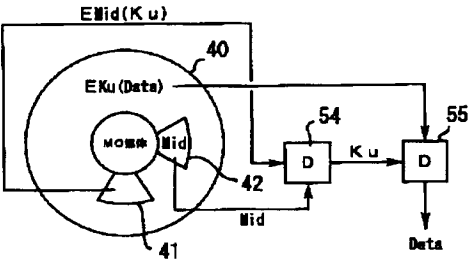
【図6】



【図8】



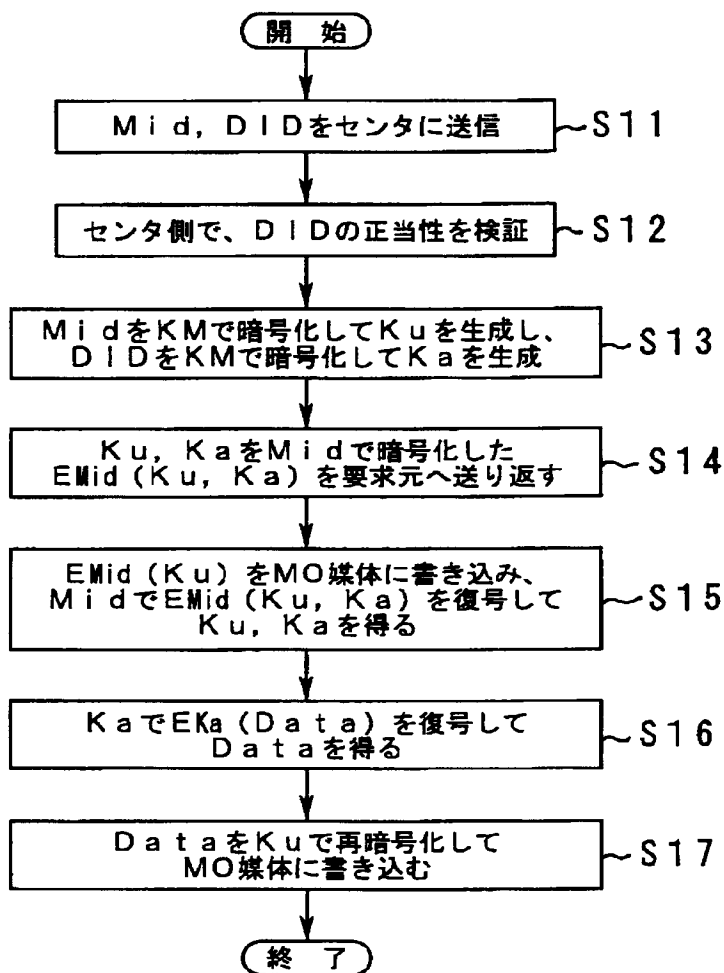
【図10】



(11)

特開平10-83297

【図7】



【図9】

